

Special Issue
International Workshop on Coding and
Cryptography (WCC 2001)

Guest-Editor:
Claude Carlet

Contents

<i>C. Carlet</i> Preface	1
<i>T. Abualrub and R. Oehmke</i> Cyclic codes of length 2^e over Z_4	3
<i>T. Berger and V.I. Levenshtein</i> Application of cover-free codes and combinatorial designs to two-stage testing	11
<i>T. Blackford</i> Cyclic codes over Z_4 of oddly even length	27
<i>C. Blundo, P. D'Arco and C. Padró</i> A ramp model for distributed key distribution schemes	47
<i>Y. Borissov, N. Manev and S. Nikova</i> On the non-minimal codewords in binary Reed–Muller codes	65
<i>G. Cohen, S. Encheva, S. Litsyn and H.G. Schaathun</i> Intersecting codes and separating codes	75
<i>D. Danev</i> Some constructions of superimposed codes in Euclidean spaces	85
<i>C. Ding and C. Xing</i> Several classes of $(2^m - 1, w, 2)$ optical orthogonal codes	103
<i>S.T. Dougherty, T.A. Gulliver and M. Oura</i> Higher weights and graded rings for binary self-dual codes	121

<i>J.I. Farrán and C. Munuera</i> Goppa-like bounds for the generalized Feng–Rao distances	145
<i>F.-W. Fu, T. Kløve, Y. Luo and V.K. Wei</i> On equidistant constant weight codes	157
<i>S.D. Galbraith</i> Weil descent of Jacobians	165
<i>L.R. Knudsen and C.J. Mitchell</i> Analysis of 3gpp-MAC and two-key 3gpp-MAC	181
<i>T. Lange and A. Winterhof</i> Interpolation of the discrete logarithm in \mathbf{F}_q by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$	193
<i>A.V. Ourivski and E.M. Gabidulin</i> Column scrambler for the GPT cryptosystem	207
<i>C. Padró, I. Gracia, S. Martín and P. Morillo</i> Linear broadcast encryption schemes	223
<i>G. Sáez</i> Generation of key predistribution schemes using secret sharing schemes	239
<i>H.G. Schaathun and W. Willems</i> A lower bound on the weight hierarchies of product codes	251
<i>K. Shiromoto and L. Storme</i> A Griesmer bound for linear codes over finite quasi-Frobenius rings	263
<i>G. Skersys</i> The average dimension of the hull of cyclic codes	275
<i>E. Soljanin and E. Oer</i> Bit-optimal decoding of codes whose Tanner graphs are trees	293
<i>H. Tapia-Recillas and G. Vega</i> Some constacyclic codes over \mathbb{Z}_{2^k} and binary quasi-cyclic codes	305